State of Colorado
Cyber Security Policies

Change Control

Overview

This policy document is part of the State of Colorado Cyber Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Agencies within the scope of this Policy must support and comply with the Requirements section of this document. Additional best-practice guidance is outlined in the Guidelines Section which has been designed to help an Agency achieve the objective of this Policy.

For the purposes of this document, an "Agency" includes organizations as defined in C.R.S. 24-37.5-102(5).

Authority

C.R.S. 24-37.5-401(1), C.R.S. 24-37.5-403(2)(b)-(c), C.R.S. 24-37.5-404(2)(b).

Scope

This policy document applies to every State agency ("Agency") as defined in C.R.S. 24-37.5-102(5). "State agency" means every state office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "State agency" does not include State-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof.

Policy

All Agencies shall develop, disseminate, implement and periodically review a formal documented Configuration Management and Change Control Program that addresses purpose, scope, roles, responsibilities, and compliance with regulations and this policy. In addition the agency is to develop and enforce formal, documented procedures to facilitate the implementation of the Configuration Management and Change Control Program.

Definitions

System Owner: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system and the information it contains.

Configuration Management: - is the process for consciously configuring hardware, firmware, software, and documentation to ensure the information system is protected against improper use or unintended failure before, during and after system implementation.

Change Control: - is the process for controlling modifications to hardware, firmware, software and documentation to ensure the information system is consistently available to users and the system and data it contains are protected from improper modifications before, during, and after the system implementation.

Change Control Authority (Board): - is an individual or group with authority to approve or disapprove changes to the system.

For the purposes of this document, please refer to C.R.S. 24-37.5-102, C.R.S 24-37.5-402 and the Colorado Cyber Security Program Policy Glossary for any terms not specifically defined herein.

Roles and Responsibilities

Agency Executive Director - responsible for:

- Approving the establishment of a change approval authority with cross-functional membership
- Delegating authority to the Agency Chief Information Officer (CIO) for appointing members to the change approval authority.

Agency CIO - is responsible for:

- Reviewing and approving the Agency change control procedures.
- Appointing members of the Change Control authority.

Agency Information Security Officer (ISO) – is responsible for monitoring the effectiveness of the change control process through periodic formal or informal audits.

Agency IT staff – is responsible for adhering to the change control process in the course of performing job duties.

Requirements

Each Agency shall implement a documented change control process and have it approved by the Agency CIO. This process must contain, at a minimum:

- An inventory of the critical systems, their components, and the baseline configuration of those components. This inventory is to be maintained to always reflect the current state.
- System changes must be documented and approved in advance by a Change Control Authority, as designated by the Executive Director.
- Configuration Management documentation must be updated to reflect the current state of the system once any change has occurred.

- System changes must be applied only by authorized personnel.
- The Change Control procedures in place within the Agency must contain provisions for emergency system changes and approval or documentation of the change after the emergency change has been implemented.
- Changes made to security devices by one individual must be reviewed by another similarly-qualified individual. "Similarly qualified" may be defined by the Agency at their discretion.
- Prior to approving changes, the Agency conducts a Cyber Security risk analysis to ensure that the availability, confidentiality and integrity of the system and the data it contains are maintained during and as a result of the proposed change.
- For changes to Major Systems must be tested for security control effectiveness prior to implementing the change in a production environment.
- A process for auditing the effectiveness is to be conducted at least once a year.

Guidelines

This section describes best practices for meeting the objective of this policy.

Change Control Process

All change control processes are to include the following:

- An analysis to specify requirements and prioritize the timing and methodology to implement changes based upon the business need. The change control process is to accommodate immediate updates to remediate system vulnerabilities and implement required virus protection while at the same time accommodating systematic architectural changes to critical systems or applications.
- A risk assessment to identify controls required to be maintained or added to meet risk control and security objectives.
- Approval by the Agency ISO and system owner.
- A back-out plan.
- Security and operational test objectives and results.
- Updated operating guides affected by the change.
- An automated process to ensure that unauthorized changes to critical devices are detected and alarmed automatically, or at a minimum, that all changes are logged and the logs are reviewed on a regular basis.
- Enforceable disciplinary consequences for making unauthorized changes to critical systems.
- An automated mechanism to document proposed changes, notify appropriate approval authorities, inhibit changes that have not been approved, and document changes that have been made.
- The annual audit requirement is to be part of the annual self-assessment process in accordance with the Colorado Cyber Security Plan (CCSP) Security Review and Audit procedures.

Network, Access Control Servers and Security Device Change Control

The Local Area Network (LAN) and Wide Area Network (WAN) are critical components for delivering reliable service to end users, as are servers that provide user authentication or control access. These devices along with firewalls and other access controlling security devices are to follow the guidelines below. The Agency firewalls are a gateway that limits access between networks. All traffic between trusted and un-trusted networks must route through it, and only authorized traffic is allowed to pass. Authorized traffic may change according to business needs and any change must be analyzed for any possible security implications.

- Changes to the production firewalls, network devices and access control servers are to be replicated on a backup device (as applicable to the Agency) to maintain configuration integrity in the event of failure of the production devices.
- All changes to the network, security, or access control device are to be reviewed by two administrators in the IT department.
- Access to devices to make configuration changes are to be limited by automated devices.
- All changes to these devices are to be logged and the logs are to be reviewed routinely, or alarmed to alert administrators to unauthorized changes.

Configuration Standards

All devices are to be configured to allow the least access necessary for the functions required for normal operation.

References

- ISO 17799-2005
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems"